



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/910,368	07/20/2001	Takumi Okaue	SONYJP 3.0-189	4307

530 7590 12/20/2005
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER

LASHLEY, LAUREL L

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/910,368	Applicant(s) OKAUE ET AL.	
	Examiner Laurel Lashley	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07/20/2001 and 02/19/03 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☒ Certified copies of the priority documents have been received in Application No. P2000-222122.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 29 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. JAPAN P2000-222122, filed on 07/24/2000. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 11/01/04 was filed after the mailing date of the application on 07/24/2001. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

4. The drawings were received on 07/20/2001 and 02/19/2003. These drawings are accepted.

Claim Objections

5. Claim 2 is objected to because of the following informality:
 - Recitation of "lower-ran key", which should be --lower-rank key--.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2132

6. Claims 1 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claims 1 and 13 recite the limitations "said contents data". There is insufficient antecedent basis for this limitation in the claim.
- Claims 2 and 14 recite the limitations "said key tree". There is insufficient antecedent basis for this limitation in the claim. Furthermore, claim 2 recites the additional limitations "said individual leaves" and "said enabling key block". Similarly, there is insufficient antecedent basis for this limitation in the claim.
- Claim 4 recites the limitation "said header". There is insufficient antecedent basis for this limitation in the claim.
- Claim 5 recites the limitation "said reproduction apparatus". There is insufficient antecedent basis for this limitation in the claim.
- Claim 15 recites the limitation "said enabling key block distribution key enciphering key". There is insufficient antecedent basis for this limitation in the claim.
- Claim 19 recites the limitation "said corresponding contents data". There is insufficient antecedent basis for this limitation in the claim.
- Claim 23 recites the limitation "said acquired contents key". There is insufficient antecedent basis for this limitation in the claim.
- Claim 24 recites the limitation "said corresponding data processing apparatus". There is insufficient antecedent basis for this limitation in the claim.

- Claim 29 recites the limitation "said preceding step". There is insufficient antecedent basis for this limitation in the claim.

The 112, second paragraph objections discussed are exemplary. Appropriate correction is required throughout the entire application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 1, 13, 19, and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Bell et al. in US Patent 6,832,319 (hereinafter US '319).

8. Regarding claims 1, 13, 19 and 29 as taught by Bell et al. which discloses as a system, method, apparatus, and program providing medium respectively:

a contents ciphering key applicable to a contents ciphering process as a header data corresponding to said contents data and then executes a process for ciphering the corresponding contents data by applying said contents ciphering key contained in said header data; wherein

said header data comprises a plurality of ciphered contents ciphering key generated by said contents ciphering key respectively ciphered by applying mutually different key ciphering key (see US '319: column 2, lines 52 – 65: where the content key is equivalent to the contents ciphering key and processes are equivalent to instance case).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 2 – 12, 14 – 18, 20 – 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bell et al. in US Patent 6,832,319 (hereinafter US '319) in view of Caronni et al. in US Patent 6,049,878 (hereinafter US '878).

As it relates to claims 2, 14 and 20, as taught by Bell et al. in US '319, which discloses as a system and method respectively:

an updating key (see US '319: column 3, lines 1 – 3: as performed by the exchange key);

and

a storage key proper to individual storage device for storing contents data (see US '319: column 3, lines 15 – 16: as performed by the bus content key)

and implies

an enabling key block distribution key enciphering key (see US '319: column 2, lines 47 and 50: as performed by media key block and media key respectively)

but does not teach

on such path for constituting a key tree structure comprising of a plurality of keys disposed in correspondence with a plurality of roots, nodes, and leaves on said paths ranging from said roots to said leaves of said key tree, wherein said individual leaves comprise a plurality of devices

or expressly state

an enabling key block distribution key enciphering key respectively comprising of key enciphering key ciphered by said enabling key block containing such data for ciphering upper-rank key by means of lower-ran key.

Caronni et al. in US '878 does teach:

on such path for constituting a key tree structure comprising of a plurality of keys disposed in correspondence with a plurality of roots, nodes, and leaves on said paths ranging from said roots to said leaves of said key tree, wherein said individual leaves comprise a plurality of devices

and expressly states:

an enabling key block distribution key enciphering key respectively comprising of key enciphering key ciphered by said enabling key block containing such data for ciphering upper-rank key by means of lower-ran key (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claims 2, 14 and 20, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Bell et al. and Caronni et al. as they both use features of key management within the same field of endeavor (safely and securely distributing keys) and with the same problem sought to be solved (preserving the security of data and achieving high efficiency in data processing).

As it pertains to claims 3, 15 and 21, Caronni et al. in view of Bell et al. teaches as a system, method and apparatus respectively:

each of said enabling key block containing said enabling key block distribution key enciphering key is so structured that, among a plurality of devices constituting leaves of said key tree structure, only such properly licensed devices are enabled to decode said enabling key block, whereas such improper devices devoid of a proper license are unable to decode said enabling key block (see US '319: column 3, lines 41 – 50).

Relating to claims 4, 16 and 22, Caronni et al. in view of Bell et al. teaches as a system, method and apparatus respectively:

an identification data for discerning actual storage or absence of storage of said enabling key blocks (see US '319: column 2, lines 44 – 46).

For claim 5, Caronni et al. in view of Bell et al. (interpreted by examiner in terms of Claim 2) teaches as a system:

a storage device for storing said header data and such contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17) and

a plurality of reproduction apparatuses for reproducing such contents data stored in said storage devices; wherein

said reproduction apparatus selects one of said ciphered plural contents ciphering keys to execute a process for ciphering said contents data (see US '319: Figure 1, item 20: recorder: and column 5, line 35).

Relating to claim 6, Bell et al. in view of Caronni et al. teaches:
said enabling key block distribution key enciphering key to be provided after being ciphered by

said enabling key block is subject to control of a version to enable a process for renewing every version to be executed (US '878: see column 6, line 66 – column 7, lines 1 – 6).

For claim 7 as taught by Bell et al. in US '319 which discloses:
a storage device for storing contents data and such contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17)

a plurality of reproduction apparatuses for reproducing a contents data stored in said storage device; (see US '319: Figure 1, item 20: recorder: and column 5, line 35) wherein
and

stores said ciphered storage key in a memory means inside of each of said reproduction apparatuses (see US '319: column 3, lines 41 – 50)

but does not disclose

one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses as own leaves and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each reproduction apparatus ciphers a specific leaf-key disposed in correspondence with own leaves by means of a storage key proper to the reproduction apparatus.

Caronni et al. in US '878 however, does show:

one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses as own leaves and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each reproduction apparatus ciphers a specific leaf-key disposed in correspondence with own leaves by means of a storage key proper to the reproduction apparatus (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 7, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor (safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (reduction/contraction of message volume).

As for claim 8, as taught by Bell et al. in US '319 which discloses:

a storage device for storing said header data and such contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17) and

a plurality of devices for reproducing a contents data stored in said storage device; (see US '319: Figure 1, item 20: recorder: and column 5, line 35)

but does not show

wherein each of said devices functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of devices as own leaves and containing a variety of keys set in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, each of said devices stores such a leaf identification element set in correspondence with own leaves in a memory means inside of each of said reproduction apparatuses.

Caronni et al. in US '878 however, does disclose:

wherein each of said devices functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of devices as own leaves and containing a variety of keys set in correspondence with roots,

nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, each of said devices stores such a leaf identification element set in correspondence with own leaves in a memory means inside of each of said reproduction apparatuses (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 8, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor (safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (reduction/contraction of message volume).

For claim 9, as taught by Bell et al. in US '319 which discloses:

a storage device for storing said header data and a contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17) and

a plurality of reproduction apparatuses individually reproducing a contents data stored in said storage device; (see US '319: Figure 1, item 20: recorder: and column 5, line 35)

and

then stores said ciphered storage key in a memory means inside of a corresponding reproduction apparatus; (see US '319: column 3, lines 41 – 50)

but does not disclose

wherein each of said reproduction apparatuses functions itself as one of leaves of said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each of said reproduction apparatuses ciphers such a leaf-key disposed in correspondence to own leaves by applying a storage key proper to each reproduction apparatus,

and

wherein said storage key proper to each reproduction apparatus is generated based on a leaf-identifying element of a leaf component corresponding to each reproduction apparatus present in said key tree structure.

Caronni et al. in US '878 however, does disclose:

wherein each of said reproduction apparatuses functions itself as one of leaves of said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure,

each of said reproduction apparatuses ciphers such a leaf-key disposed in correspondence to own leaves by applying a storage key proper to each reproduction apparatus,

and

wherein said storage key proper to each reproduction apparatus is generated based on a leaf-identifying element of a leaf component corresponding to each reproduction apparatus present in said key tree structure (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 9, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor

(safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (reduction/contraction of message volume).

As it pertains to claim 10, US '319 teaches:

a storage device for storing said header data and such contents data disposed in correspondence with said contents data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17)

a plurality of reproduction apparatuses individually reproducing contents data stored in said storage device; (see US '319: Figure 1, item 20: recorder: and column 5, line 35)

but does not teach

wherein each of said reproduction apparatuses functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, based on a leaf key set in correspondence with own leaves, stores a device key block in a memory means inside of each reproduction apparatus, wherein said device key block comprises an assemblage of ciphered keys comprising plural steps of node keys which are disposed on such paths ranging from own leaves up to upper rank keys of said key tree structure and individually ciphered.

Caronni et al. in US '878 however, does disclose:

wherein each of said reproduction apparatuses functions itself as one of leaves for constituting said key tree structure by way of the following: initially, among a key tree structure comprising a plurality of reproduction apparatuses and containing a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure, based on a leaf key set in correspondence with own leaves, stores a

device key block in a memory means inside of each reproduction apparatus, wherein said device key block comprises an assemblage of ciphered keys comprising plural steps of node keys which are disposed on such paths ranging from own leaves up to upper rank keys of said key tree structure and individually ciphered (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 10, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor (safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (reduction/contraction of message volume).

For claim 11, US '319 teaches:
a storage device for storing said header data and such contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk and column 6, lines 16 – 17)
but does not disclose

a plurality of reproduction apparatuses for reproducing said contents data stored in said storage device; wherein each of said reproduction apparatuses stores a plurality of initial enabling key blocks in a memory means inside of each reproduction apparatus; wherein each of said initial enabling key blocks comprises a plurality of keys on such paths for constituting a key tree structure consisting of a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of reproduction apparatuses as own leaves.

Caronni et al. in US '878 however, does disclose
a plurality of reproduction apparatuses for reproducing said contents data stored in said storage device; wherein each of said reproduction apparatuses stores a plurality of initial

enabling key blocks in a memory means inside of each reproduction apparatus; wherein each of said initial enabling key blocks comprises a plurality of keys on such paths for constituting a key tree structure consisting of a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of reproduction apparatuses as own leaves (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 11, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor (safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (reduction/contraction of message volume).

In addressing claim 12, Bell et al. in view of Caronni et al. teaches:
each of said initial enabling key block is commonly stored in such a device belonging to lower-rank of a plurality of category nodes disposed at a predetermined step of said key tree structure (see US '878: column 6, lines 20 – 46).

For claims 17 and 23, Caronni et al. in view of Bell et al. (interpreted by examiner in terms of claim 14 and 20 respectively) teaches:

wherein, in the process for reproducing a contents data from a storage device storing said header data and such a contents data disposed in correspondence with said header data,
said data processing method selects one of said ciphered plural contents ciphering keys to acquire a proper contents ciphering key before eventually decoding said contents data by applying said acquired contents ciphering key (see US '319: Figure 3, item 32: disk, column 6, lines 16 – 17 and Figure 1, item 20: recorder, column 5, line 35).

As for claim 18, US '319 teaches:
wherein, in the process for reproducing a contents data from a storage device storing said

header data and such a contents data disposed in correspondence with said header data, (see US '319: Figure 3, item 32: disk, column 6, lines 16 – 17)

and

a device key block processing step for acquiring a specific node key via a process for decoding a device key block comprising an assemblage of ciphered keys consisting of plural steps of individually ciphered mutually different node keys on such paths ranging from own leaves up to upper-rank keys of said key tree structure; and

a final step of processing said enabling key blocks based on the acquired node key (see US '319: column 3, lines 17 – 39)

but does not teach

said data processing method executes serial processing steps including the following: initially, based on such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys set in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices as own leaves, said data processing method executes.

Caronni et al. in US '878 however, does disclose

said data processing method executes serial processing steps including the following: initially, based on such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys set in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices as own leaves, said data processing method executes (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claim 18, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor

(providing a management structure to safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (negate the need for mutual authentication among authorized users).

For claims 24 – 28, as taught by US '319 disclose

such a system for reproducing such a contents data stored in a storage device for storing said header data and such a contents data disposed in correspondence with said header data; (see US '319: Figure 3, item 32: disk, column 6, lines 16 – 17 and Figure 1, item 20: recorder, column 5, line 35) and

but fails to teach

such a system which enables such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be ciphered by a storage key proper to said data processing apparatus and then stored in a memory means inside of said corresponding data processing apparatus

or

such a system for enabling an initial enabling key block comprising a plurality of keys ciphered by means of lower rank keys on such paths for constituting a key tree structure comprising a variety keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from root to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be stored in said corresponding data processing apparatus.

Caronni et al. in US '878 however, does disclose

such a system which enables such a leaf-key disposed in correspondence with own leaves among a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be ciphered by a storage key proper to said data processing apparatus and then stored in a memory means inside of said corresponding data processing apparatus
and

such a system for enabling an initial enabling key block comprising a plurality of keys ciphered by means of lower rank keys on such paths for constituting a key tree structure comprising a variety keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from root to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves to be stored in said corresponding data processing apparatus (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46).

For claims 24 – 28, it would be obvious to one of ordinary skill in the art at the time of the invention as they both use features of key management within the same field of endeavor (providing a management structure to safely and securely distributing keys that provide access to data) and with the same problem sought to be solved (negate the need for mutual authentication among authorized users).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is US Patent 4,386,234 as anticipated by Ehrtam et al.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

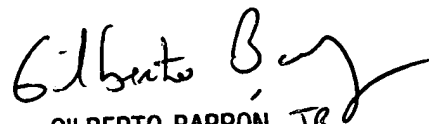
Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Laurel Lashley
Examiner
Art Unit 2132

 08 December 2005
LLL


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100